



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Chairman

May 7, 2004

The Honorable Edward J. Markey
United States House of Representatives
Washington, DC 20515-2107

Dear Congressman Markey:

Thank you for your letters relating to the protection of personal information of American citizens when that information is processed outside the United States. I am pleased to have this opportunity to answer your questions about the privacy laws and rules enforced by the Federal Trade Commission ("Commission"), including the Children's Online Privacy Protection Act, the Do Not Call Registry, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act.

The Commission considers privacy one of the central elements of its consumer protection mission. As you know, under the Federal Trade Commission Act, the Commission may use its authority to stop unfair or deceptive acts or practices involving the privacy and confidentiality of personal consumer information.¹ Under the Gramm-Leach-Bliley Act,² the Commission has implemented rules requiring financial privacy notices³ and reasonable, administrative, technical, and physical safeguards of personal information.⁴ The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act. In addition, the recently amended Telemarketing Sales Rule established the National Do Not Call Registry, which allows consumers to reduce the number of unwanted telemarketing sales calls.

Your letters raise the question of how these protections apply if personal information of consumers is transferred to off-shore locations for processing, including billing, customer service, call center, or other support services. A company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws. Simply because a company chooses to outsource some of its data processing to a domestic or off-shore service provider does not allow that company to escape liability for any failure to safeguard the information adequately. In those situations, the Commission would look to whether the

¹See, e.g., Microsoft Corp., FTC Dkt. No. C-4069 (Dec. 20, 2002) (alleging that security claims were deceptive where company failed to undertake reasonable and appropriate measures under the circumstances to ensure adequate security).

²15 U.S.C. §§ 6801-6809 (2004)

³16 C.F.R. § 313 (2004) (The Financial Privacy Rule).

⁴16 C.F.R. § 314 (2004) (The Safeguards Rule).

company that outsourced the data processing employed sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information.⁵

I address your specific questions below beginning with those posed in your letter to the Federal Trade Commission and Federal Communications Commission followed by those in your letter to the FTC and the GLB agencies.

Children's Online Privacy Protection Act of 1998 (COPPA)

Congress passed COPPA in October 1998, with a requirement that the Commission issue and enforce rules concerning children's online privacy. The Commission issued the final COPPA Rule (the "Rule") in November 1999, and the Rule went into effect in April 2000. As a general matter, the Rule requires that website operators must obtain verifiable parental consent before collecting personal information from children under the age of 13.⁶ In addition, the Rule places a responsibility on website operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."⁷

The Rule does not prohibit website operators from disclosing children's personal information to off-shore companies for processing. Website operators are permitted to contract with agents located domestically or off-shore to perform processing on the website operator's behalf. Nevertheless, as part of the website operator's requirement to establish and maintain reasonable procedures⁸ to protect the children's personal information, the website operator, when

⁵You asked whether individuals have a private right of action under specific laws enforced by the Commission. There is no private right of action under the Federal Trade Commission Act, the Children's Online Privacy Protection Act, or the Gramm-Leach Bliley Act. The Fair Credit Reporting Act provides for a private right of action for most violations of the Act, including a negligent or willful disclosure of a consumer report in violation of the Act. Many state laws provide individuals with a private right of action for many of the acts and practices that would violate state laws similar to those laws enforced by the Commission.

⁶The Rule applies to operators of commercial websites and online services directed to children under 13 that collect personal information from children, and operators of general audience sites with actual knowledge that they are collecting information from children under 13.

⁷16 C.F.R. § 312.8 (2004).

⁸See Statement of Basis and Purpose, 64 Fed. Reg. 59,888, 59,906 (1999) (procedures for complying with this provision could include "using secure web servers and firewalls; deleting personal information once it is no longer being used; limiting employee access to data and providing those employees with data-handling training; and carefully screening the third parties

choosing to have processing done by an agent on the website operator's behalf, must take appropriate measures to ensure that its agent is adequately safeguarding the children's personal information. A failure by the website operator to ensure that its agents have reasonable procedures in place could result in a finding that the website operator violated COPPA. It would make no difference whether its agents were foreign or domestic entities.

You also asked whether COPPA applies to website operators located outside the United States. Foreign-run websites that are directed to children in the United States or knowingly collect information from children in the United States must also comply with COPPA. For example, foreign-run child-oriented websites would be subject to COPPA if they advertised in offline media in the United States or on popular United States websites.⁹ The Rule does not distinguish between domestic websites and foreign-run websites for purposes of COPPA compliance and enforcement.¹⁰

Do-Not-Call Registry

The Commission issued the amended Telemarketing Sales Rule (TSR) on January 29, 2003. Like the original 1995 TSR, the amended TSR gives effect to the Telemarketing and Consumer Fraud and Abuse Prevention Act. This legislation gives the Commission and state attorneys general law enforcement tools to combat telemarketing fraud and gives consumers added privacy protections and defenses against unscrupulous telemarketers. One significant amendment to the TSR prohibits the making of certain telemarketing calls to consumers who have put their phone numbers on the National Do Not Call Registry.

You asked three specific questions about the Do Not Call Registry. First, you asked whether telemarketers are relocating outside the United States. Based on our telemarketing law enforcement and rulemaking activities, I am aware of a long-term trend of firms moving their telemarketing operations to locations outside the United States for a number of reasons, including the lower cost of overseas operations. I am unaware, however, of any specific indicators suggesting that the establishment of the Do Not Call Registry has prompted telemarketing firms to relocate off-shore or accelerated this trend.

to whom such information is disclosed").

⁹The Rule's definition of an "operator" – which is subject to the Act – includes foreign websites that are involved in commerce in the United States or its territories. 16 C.F.R. §312.2 (2004).

¹⁰ In certain situations, rather than initiating an enforcement action, the Commission will provide the operator with guidance on how to become COPPA-compliant. The Commission has provided guidance to many operators, including several foreign-run websites, to assist them in becoming COPPA-compliant.

In response to your second question, the amended TSR, including the Do Not Call provisions, applies to *all* sellers and telemarketers that call consumers in the United States, including sellers and telemarketers operating off-shore. Importantly, if a domestic seller hires an off-shore telemarketer to call United States consumers on the domestic seller's behalf, the domestic seller (as well as the off-shore telemarketer) may be held liable for violations of the Do Not Call provisions of the TSR. Compliance with the Do Not Call Registry has been excellent.¹¹

Your third question asks whether the Commission has brought enforcement actions against off-shore telemarketers. Since 2000, the Commission has brought actions against foreign defendants in approximately 50 consumer protection cases and provided redress to thousands of United States and foreign consumers. For example, in 2001, the Commission, alleging violations of the TSR, brought an enforcement action against a foreign-based telemarketer who cold-called tens of thousands of United States consumers in an attempt to sell them bogus identity theft protection services and supposed advance-fee, low-interest credit cards. Under the terms of the settlement reached in 2002, the foreign telemarketer paid over \$111,000 in consumer redress.¹²

The Gramm-Leach-Bliley Act and the Fair Credit Reporting Act

As you know, eight federal agencies and the states have authority to implement the GLB Act provisions with respect to financial institutions under their jurisdiction, and all have issued consistent and comparable regulations to carry out these provisions.¹³ In your letter to the FTC

¹¹See www.ftc.gov/opa/2004/02/dncstats0204.htm (February 2004 press release stating that Do Not Call registration and complaint figures for 2003 indicate that fewer than 45 companies have received more than 100 consumer complaints. Consumers registered over 55 million numbers through 2003, but reported only 150,000 possible violations.). Nevertheless, the Commission will be vigilant regarding companies that violate the Do Not Call rules. See *FTC v. National Consumer Council*, No. SACV 04-0474 CFC (JWJx) (C.D. Cal. Western Div. May 3, 2004), the Commission's first action enforcing the TSR's National Do Not Call Registry. See www.ftc.gov/opa/2004/05/ncc.htm (May 5, 2004 press release regarding case).

¹²*FTC v. R & R Assocs., Inc.*, No. 01-CV-1537 TJM (N.D.N.Y. Apr. 25, 2002).

¹³ The Commission issued two regulations to carry out the statutory requirements of the GLB Act: the Financial Privacy Rule (Privacy Rule) and the Safeguards Rule. Both Rules apply to "financial institutions," defined as entities that engage in certain "financial activities" identified in section 4(k) of the Bank Holding Company Act and implementing regulations. 15 U.S.C. § 6809(3) (2004); 16 C.F.R. § 313.3(k) (2004). This broad definition includes traditional financial institutions such as banks, securities firms, and insurance companies, as well as a wide array of other financial institutions that, under the Commission's Rules, are "significantly engaged" in such financial activities. These include, for example, non-bank lenders, loan brokers, financial or investment advisors, tax preparers, real estate settlement services, debt collectors, and credit bureaus.

and the GLB agencies, you asked specific questions about the application of financial privacy laws when companies subject to those laws transfer nonpublic personal financial information to off-shore entities. As a general matter, under these laws, financial institutions do not have to disclose to consumers that they are sharing nonpublic personal information with service providers.¹⁴ Nevertheless, financial institutions are responsible for ensuring that certain service providers maintain the confidentiality of that information.

The *GLB Safeguards Rule* squarely addresses the situation you posit because it imposes an express duty on financial institutions to protect customers' nonpublic personal information that is shared with service providers.¹⁵ This is true regardless of whether the service provider is located in the United States or overseas, or whether the service provider is an affiliate or a nonaffiliated third party. Specifically, the Safeguards Rule requires all financial institutions to design, implement, and maintain an information security program to safeguard customer information.¹⁶ As part of the information security program, financial institutions must oversee service providers (whether domestic or off-shore) by: (a) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards; and (b) requiring service providers by contract to implement and maintain such safeguards. If a financial institution failed to take these required steps with respect to its service provider, and the service provider failed to safeguard the customer information, there could be a finding that the financial institution violated the Safeguards Rule. Thus, in the example you posed regarding the actions of a rogue employee of a service provider, the Safeguards Rule would impose liability on a financial institution if it failed to undertake appropriate measures to ensure that its service providers were providing appropriate safeguards, including training and screening of employees. The Commission's general authority under Section 5 of the FTC Act also reaches this conduct.

The *Fair Credit Reporting Act* (FCRA) promotes fairness, privacy, and accuracy in the consumer credit marketplace. Under the FCRA, consumer reporting agencies, including credit bureaus, are required to maintain reasonable procedures to ensure that consumer reports are

¹⁴The *GLB Privacy Rule* requires financial institutions to give their customers privacy notices that describe the financial institution's information collection and sharing practices. Financial institutions are not required to describe in the notice the specific identity or location of companies with which they are sharing information. In certain circumstances, however, the Rule requires notice to consumers about sharing information with service providers as well as a contract with those service providers to protect the confidentiality of the information.

¹⁵16 C.F.R. § 314.4(d) (2004). The duty to protect customer information also applies to information handled or maintained by the financial institution's affiliates. 16 C.F.R. 314.2(b).

¹⁶15 U.S.C. § 6801(b) (2004). The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit bureaus – that receive customer information from other financial institutions.

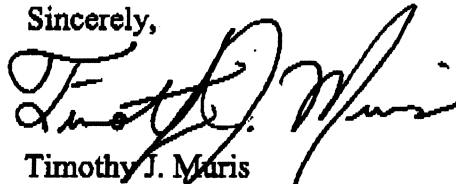
furnished only to those with a permissible purpose as set forth in the Act.¹⁷ Although the FCRA does not prohibit a consumer reporting agency from using off-shore contractors, the consumer reporting agency may be liable if it failed to take appropriate steps to ensure that its agents (whether located domestically or off-shore) had reasonable procedures to protect consumer report information in accordance with the FCRA.

You also asked for specific information about the companies that transfer personal consumer information off-shore and the categories of personal consumer information transferred by these companies. The numerous and varied entities subject to the Commission's jurisdiction do not report this information to the Commission, nor would it be practical to require them to do so.

Thus far, the agency has not brought a law enforcement action based on the failure of a service provider – here or overseas – to protect information. The Commission has conducted and continues to conduct nonpublic investigations of companies' compliance with the Privacy Rule and the Safeguards Rule; as part of these investigations, the Commission routinely asks about companies' relationships with service providers.

Thank you for the opportunity to provide you with this information.

Sincerely,

A handwritten signature in black ink, appearing to read "Timothy J. Muris", written over a horizontal line.

Timothy J. Muris
Chairman

¹⁷15 U.S.C. § 1681e.